Commonwealth of Kentucky
Public Protection Cabinet

Steve Beshear, Governor **Robert D. Vance, Secretary**

FOR IMMEDIATE RELEASE

Contact: Kelly May
502-573-3390 x252
800-223-2579 x252
502-229-5068 Cell
kelly.may@ky.gov

Guard Against Phishing in Wake of Heartbleed Bug

Department of Financial Institutions Urges Caution

FRANKFORT, Ky. (April 15, 2014) – With reports of the Heartbleed bug spreading like wildfire, it's important to stay vigilant against potential scams.

The Department of Financial Institutions (DFI) is warning consumers about possible phishing attempts in the wake of the Heartbleed bug – a critical security vulnerability that has put many systems at risk.

"Con artists often take advantage of hot topics in the news," said DFI Commissioner Charles Vice. "Consumers will become prime targets for phishing attempts to change passwords or account information. Protect against phishing by avoiding links in emails you did not request and dealing only with websites and companies you trust."

Businesses or websites using affected versions of OpenSSL encryption should be working to update their systems to fix this vulnerability. Those businesses may suggest people change their passwords to protect both the customers and the business. As sites are patched and are no longer vulnerable, consider changing passwords. Choose strong passwords and use a different password on each site. For more tips on passwords and other security issues, visit OnGuardOnline: http://www.onguardonline.gov/articles/0009-computer-security.

However, people should be wary of links in email notices as these could be phishing attempts. Phishing is the use of fraudulent email to acquire sensitive information, such as passwords and financial account details. Phishing e-mails appear to be from legitimate sources, such as banks or online services. Often the link will lead to a false website that looks identical to the company's real site, luring the consumer to reveal logon credentials or other personal information to cybercriminals.

Also beware of other possible scams, such as services that offer to scan for and repair vulnerabilities on your computer. Research any service provider you plan on using to make sure it is a legitimate business before turning over any money or information.

The Financial Cybercrime Task Force of Kentucky is a proactive, internal work group of DFI that focuses on best practice guidance and warnings for the financial services industry and its customers. The Task Force's goal is to identify and address emerging threats in cybercrime and security and to protect the integrity of the Kentucky financial system.

DFI, http://kfi.ky.gov, is an agency in the Public Protection Cabinet. For more than 100 years it has supervised the financial services industry by examining, chartering, licensing and registering various financial institutions, securities firms and professionals operating in Kentucky. DFI's mission is to serve Kentucky residents and protect their financial interests by maintaining a stable financial industry, continuing effective and efficient regulatory oversight, promoting consumer confidence, and encouraging economic opportunities.

###